

## CLAIMS

What is claimed is:

- 1 1. A method for managing a secure network boot of a server blade, the server blade being in  
2 a blade chassis that has multiple server blades, the blade chassis including a switching means  
3 allowing the server blade to communicate with a network, the method comprising:  
4 storing a list of trusted management servers;  
5 broadcasting a request for a boot program from a server blade to a network of  
6 management servers;  
7 receiving a response to the request for the boot program at a switching means associated  
8 with the server blade, the response being from a responding management server on the network  
9 of management servers, the response containing directions to a boot program server;  
10 comparing an identity of the responding management server with the list of trusted  
11 management servers; and  
12 upon verifying that the responding management server is on the list of trusted  
13 management servers, transmitting the response from the responding management server to the  
14 server blade, and downloading a boot program from a boot program server specified by the  
15 responding management server.
- 1 2. The method of claim 1, further comprising:  
2 upon determining that the responding management server is not on the list of trusted  
3 management servers, blocking the transmittal of the response from the responding management  
4 server to the server blade.
- 1 3. The method of claim 2, further comprising:  
2 upon determining that the responding management server is not on the list of trusted  
3 management servers, generating an alert to a designated administrator server of a presence of an  
4 unauthorized management server on the network of management servers.

1     4.     The method of claim 1, wherein the switching means is an Ethernet switch.

1     5.     The method of claim 4, wherein the comparing step is performed by configuring the  
2 Ethernet switch to perform Layer 3 packet filtering to identify Pre-boot Execution  
3 Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the  
4 seven layers of the Open System Interconnection (OSI) model.

1     6.     The method of claim 1, further comprising:  
2         upon determining that the responding management server is not on the list of trusted  
3 management servers, downloading a boot program from a known trusted boot server in a secure  
4 local area network (LAN).

1     7.     The method of claim 1, further comprising:  
2         managing different types of boot program servers available to the server blade by  
3 maintaining, in an information technology services organization logically oriented between the  
4 different types of boot program servers and the server blade, a permission list of boot program  
5 servers authorized for each server blade in a server blade chassis.

1     8.     A system for managing a secure network boot of a server blade, the server blade being in  
2 a blade chassis that has multiple server blades, the blade chassis including a switching means  
3 allowing the server blade to communicate with a network, the system comprising:  
4         means for storing a list of trusted management servers;  
5         means for broadcasting a request for a boot program from a server blade to a network of  
6 management servers;  
7         means for receiving a response to the request for the boot program at a switching means  
8 associated with the server blade, the response being from a responding management server on  
9 the network of management servers, the response containing directions to a boot program server;

10 means for comparing an identity of the responding management server with the list of  
11 trusted management servers; and  
12 means for, upon verifying that the responding management server is on the list of trusted  
13 management servers, transmitting the response from the responding management server to the  
14 server blade, and downloading a boot program from a boot program server specified by the  
15 responding management server.

1 9. The system of claim 8, further comprising:

2 means for, upon determining that the responding management server is not on the list of  
3 trusted management servers, blocking the transmittal of the response from the responding  
4 management server to the server blade.

1 10. The system of claim 9, further comprising:

2 means for, upon determining that the responding management server is not on the list of  
3 trusted management servers, generating an alert to a designated administrator server of a  
4 presence of an unauthorized management server on the network of management servers.

1 11. The system of claim 8, wherein the switching means is an Ethernet switch coupled with  
2 the blade chassis.

1 12. The system of claim 11, wherein the means for comparing configures the Ethernet switch  
2 to perform Layer 3 packet filtering to identify Pre-boot Execution Environment/Bootstrap  
3 Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open  
4 System Interconnection (OSI) model.

1 13. The system of claim 8, further comprising:

2 means for, upon determining that the responding management server is not on the list of  
3 trusted management servers, downloading a boot program from a known trusted boot server in a  
4 secure local area network (LAN).

1 14. The system of claim 8, further comprising:

2 means for managing different types of boot program servers available to the server blade  
3 by maintaining, in an information technology services organization logically oriented between  
4 the different types of boot program servers and the server blade, a permission list of boot  
5 program servers authorized for each server blade in a server blade chassis.

1 15. A computer program product, residing on a computer usable medium, for managing a  
2 secure network boot of a server blade, the server blade being in a blade chassis that has multiple  
3 server blades, the blade chassis including a switching means allowing the server blade to  
4 communicate with a network, the computer program product comprising:

5 program code for storing a list of trusted management servers;

6 program code for broadcasting a request for a boot program from a server blade to a  
7 network of management servers;

8 program code for receiving a response to the request for the boot program at a switching  
9 means associated with the server blade, the response being from a responding management  
10 server on the network of management servers, the response containing directions to a boot  
11 program server;

12 program code for comparing an identity of the responding management server with the  
13 list of trusted management servers; and

14 program code for, upon verifying that the responding management server is on the list of  
15 trusted management servers, transmitting the response from the responding management server  
16 to the server blade, and downloading a boot program from a boot program server specified by the  
17 responding management server.

1 16. The computer program product of claim 15, further comprising:

2 program code for upon determining that the responding management server is not on the  
3 list of trusted management servers, blocking the transmittal of the response from the responding  
4 management server to the server blade.

- 1 17. The computer program product of claim 16, further comprising:  
2 program code for, upon determining that the responding management server is not on the  
3 list of trusted management servers, generating an alert to a designated administrator server of a  
4 presence of an unauthorized management server on the network of management servers.
- 1 18. The computer program product of claim 15, wherein the switching means is an Ethernet  
2 switch coupled with the blade chassis.
- 1 19. The computer program product of claim 18, wherein the comparing step is performed by  
2 configuring the Ethernet switch to perform Layer 3 packet filtering to identify Pre-boot  
3 Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network  
4 layer of the seven layers of the Open System Interconnection (OSI) model.
- 1 20. The computer program product of claim 15, further comprising:  
2 program code for, upon determining that the responding management server is not on the  
3 list of trusted management servers, downloading a boot program from a known trusted boot  
4 server in a secure local area network (LAN).
- 1 21. The computer program product of claim 15, further comprising:  
2 program code for coordinating different types of boot program servers available to the  
3 server blade by maintaining, in an information technology services organization logically  
4 oriented between the different types of boot program servers and the server blade, a permission  
5 list of boot program servers authorized for each server blade in a server blade chassis.